Will Our Data Be Any Safer in 2026?

by Sharon D. Nelson, Esq.

That was the question I was asked to answer at the College of Law Practice Management's 2016 Futures Conference. As part of a great legal technology panel, my answer was quick and decisive. No, it will not be.

Look how the cone of silence (check mentions of Maxwell Smart if you don't recognize the reference) around law firm breaches has shattered in 2016 alone. It turns out that law firms, even major law firms, have been breached again and again. Do we really believe that there will be any respite from the attacks?

Law firms, by their very nature, are honey pots. If you target a corporation, you may get that corporation's data, but probably not a lot of data from other companies. On the other hand, law firms hold the data of many individuals and corporations. That's what makes us such an attractive target. And our security is, in general, not as good as that of major business entities – though we are getting better.

Think about it – hackers are motivated largely by money (think insider knowledge that can be used to leverage stock market profits or ransomware, which has become increasingly profitable) and by espionage motives. These days, all nations seem to be spying on each other, also for economic motives to protect their own countries, but additionally for political and military intelligence. I can only foresee escalation in the motivation to hack.

As we have already witnessed, attacks are increasing in number and sophistication – and the good guys are always limping badly behind the bad guys. Even the good guy countries, and I hope the U.S. is one, really believe they have the absolute right to know what we are doing. The Fourth Amendment is looking more and more like a hunk of Swiss cheese.

Worse yet, our younger generation doesn't seem to care, which makes it even easier for governments to snoop without protest.

Though encryption is a lawyer's best friend, there have been recent rumblings that AES-256 (the most common strong encryption standard) may have predictable factors that will make it easier to crack. Add that to the easy ability of governments to ramp up supercomputers and we are pretty much screwed if those rumblings are accurate.

One question from the audience involved cloud computing. Roughly 50% of lawyers embrace and roughly 50% are in the "never, ever" camp. The truth is that clouds often protect confidential data far better than law firms do. And without going totally "into the weeds", there are ways that sophisticated cloud providers (whose cybersecurity talent most law firms could NEVER afford to buy) can protect data by dispersing it into segments across multiple clouds

which has to be reassembled before you can read it. Way too simple an explanation but perhaps easier to understand.

And just wait until the day when affordable quantum computing arrives. It is in its infancy now, but think of an abacus compared to one of today's supercomputers and you may be talking about something that is a billion times more powerful than our supercomputers. And that's as technical as I will get because even my eyes glaze over when I read about quantum computing. But rest assured, quantum computing will change everything we think we know about cybersecurity.

Scary? Oh yeah. Welcome to the future of trying to protect law firm data!

The author is the President of Sensei Enterprises, Inc., a legal technology, information security and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com